STATE OF IOWA

MASTER AGREEMENT

Contract Declaration and Execution

EFFECTIVE BEGIN DATE: 07-16-2008
EXPIRATION DATE: 07-15-2009

VENDOR:
Websolv Computing
Ste 240
14225 University Ave
Waukee, IA 50263
USA

VENDOR CONTACT:
ALLEN NGUYEN
PHONE: 515-453-8247 **EXT:**
EMAIL: allen.nguyen@ecfirst.com

FOB FOB Dest, Freight Allowed

ISSUER:
JEANETTE CHUPP
PHONE: 515-281-6288
EMAIL: Jeanette.Chupp@iowa.gov

Contract For: Healthcare and Information Technology Consultation.

The parties agree to comply with the terms and conditions on the following attachments which are by this reference made a part of the Agreement. Attachment 1: General Terms and Conditions for service/goods contracts posted at: http://das.gse.iowa.gov/terms_goods.pdf and http://das.gse.iowa.gov/terms_services.pdf. Certified Targeted Small Business Contract for the provision of Healthcare related services and Information Technolgoy Services as listed herein, on an as-needed basis under the authority of Iowa Code Section 18.6(8) and Administrative Rule 401-7.3(4). State of Iowa Facilities, Agencies and Departments may purchase goods and services from a Certified Targeted Small Business (TSB) in an amount up to $10,000 per purchase. Refer to the attached TSB Certificate and HIPAA information. VENDOR INFORMATION: WebSolv Computing Incorporated dba ECFIRST.COM, Contacts include LORNA L. WAGGONER, CHP, at Office Phone: 515-453-8247 ext. 17, or Fax: 515-453-8471, or E-Mail: Lorna.Waggoner@ecfirst.com, and JOANIE BOND, Account Manager at Office Phone 515-453-8247 ext. 22, or Cell Phone 515-314-8969 or E-Mail: Joanie.Bond@ecfirst.com. Project Pricing shall be quoted by individual project criteria. Approved IT Consulting Catagories of service include: 1. Strategy/Vision/Consulting, 2. Project Management, 3. Design/Planning, 4. Developing, 5. Testing, 6. Implementation, 7. Training, 8. On-Going Support, 9. Administration

RENEWAL OPTIONS

AUTHORIZED DEPARTMENT
ALL

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR		STATE OF IOWA	
CONTRACTOR'S NAME (If other than an individual, state whether a corp., partnership, etc. Websolve DBA E.C.First		AGENCY NAME Dept of Administrative Services	
BY (Authorized Signature) Joanie Bond	Date Signed 7-15-2008	BY (Authorized Signature) Jeanette Chupp	Date Signed July 14, 2008
Printed Name and Title of Person Signing Joanie Bond Business Manager		Printed Name and Title of Person Signing Jeanette Chupp	
Address 14225 Unit Ave Suite 240, Waukee IA		Address Hoover Bldg., Des Moines, Iowa	

LINE NO.	QUANTITY / SERVICE DATES	UNIT	COMMODITY / DESCRIPTION	UNIT COST / PRICE OF SERVICE
1	0.00000		948 **HEALTH RELATED SERVICES (FOR HUMAN SERVICES SEE CLASS 952)** **HEALTH RELATED SERVICES (FOR HUMAN SERVICES SEE CLASS 952)** HIPAA Security Rule Risk Analysis. HIPAA Policy and Procedure Development. HIPAA Privacy and Security Rule Audits and Consulting. HIPAA Consulting - Business Impact Analysis, Contingency Planning, Disaster Recovery. HIPAA Security Advisor Services.	$0.000000 $0.000000
2	0.00000		915 **COMMUNICATIONS AND MEDIA RELATED SERVICES** **COMMUNICATIONS AND MEDIA RELATED SERVICES** HIPPA Training - Instructor Led - ELearning, Custom Material Development.	$0.000000 $0.000000
3	0.00000		20928 **Communications: Networking, Linking, etc.** **Communications: Networking, Linking, etc.** Professional Services: Web Developers and architects, database administrators. Security Compliance Professionals and Consulting ISO17799, SOX, Cobit and others. Security Compliance Policies and Procedures. Security Audit and Evaluation. Security Compliance Advisor Services	$0.000000 $0.000000
4	0.00000		91829 **Computer Software Consulting** **Computer Software Consulting** Current Approved IT Consulting Service Catagories include: 1. Strategy/Vision/Consulting, 2. Project Management, 3. Design/Planning, 4. Developing, 5. Testing, 6. Implementation, 7. Training, 8. On-Going Support, 9. Administration. (Refer to attached information).	$0.000000 $0.000000

STATE OF IOWA

MASTER AGREEMENT

Contract Declaration and Execution

TERMS AND CONDITIONS

Terms & Conditions Goods

The parties agree to comply with the terms and conditions on the following web site which are by this reference made a part of the Agreement. General Terms and Conditions for goods contracts are posted at: http://das.gse.iowa.gov/terms_goods.pdf

Terms & Conditions Service

The parties agree to comply with the terms and conditions on the following web site which are by this reference made a part of the Agreement. General Terms and Conditions for service contracts are posted at: http://das.gse.iowa.gov/terms_services.pdf

ITQ Approved Vendor

Note: Work must still be competitively sourced per Administrative Code 11—105 & 106

Refer to Service Contracting Guide at: http://das.gse.iowa.gov/procurement/scg.html

E-Copies of Vendor's repsonse to ITQ and Cost Data is available by email: ashley.super@iowa.gov

For a copy of the ITQ (Invitation to pre-Qualify) email: ashley.super@iowa.gov

DAS
Iowa Department of
Administrative Services
General Services Enterprise

Approved IT Consulting & IT Staff Augmentation Service Provider as of Jan. 25, 2008

CATAGORIES OF SERVICE:
1. Strategy / Vision / Consulting
2. Project Management
3. Design / Planning
4. Developing
5. Testing
6. Implementation
7. Training
8. On-Going Support
9. Administration

State of Iowa

Department of Inspections and Appeals

TARGETED SMALL BUSINESS CERTIFICATION

Awarded To:

ECFIRST.COM

July, 2007

Effective Date

July, 2009

Expiration Date

Sherry Hopkins

Program Manager, Certification

Dean Lerner

Director, Department of Inspections and Appeals

Welcome to ecfirst.com

ecfirst.com

Quick Facts

- Been in the local IT sourcing business for over 10 years.
- Has a diverse team to provide a wide range of IT Services.
- Each member of the management team has at least 15 years of IT experience – all of them have worked in some role in the IT community making hiring decisions.
- Certified as a minority owned supplier.
- ecfirst will rise to a top supplier because of our quality processes and the fact that we let managers set the appropriate level of interaction and communication to help you do your job as efficiently as possible.

Distinct Differences about EC First

- All candidates are first screened by our technical recruiters and secondly by a job function specialist or independent third party firm (performed that job function or utilized that technology).
- All candidates are required to participate in our web based pre hire – 360 process (anonymous reference checking).

Advantages: Candidates are screened twice and evaluated by specialists in their field. Candidates are required to disclose past managers. Due to the anonymous feature in our product, the managers are able to quickly and confidentially disclose honest and in-depth information about the candidate's qualifications and skills.

ecfirst.com
14225 University Avenue
Suite 281
Waukee, IA 50263

"Nothing happens until I make it happen."

By Scott Wilson

Proven Track Record

- When a large, local financial firm trimmed its vendor list from 40 to 5, EC First was the only company with a Des Moines office presence to remain on the preferred list.
- EC First is rated on our ability to respond to each job order with 3 qualified candidates within 5 business days.
- We are rated by our ability to supply candidates, our ratio of qualified candidates, our interview ratio and our hire ratio.
- EC First not only qualified to be on the initial list, but have upheld the quality standards to remain on the list to date.

In 2007, ecfirst placed 69 consultants in Des Moines. Skills and average length of contract (three years data):

Skill set	% of skills placed	Avg length of contract
Java, .Net, Architects	32%	16.25 months
Business Analyst	23%	14.3 months
QA Analysts	20%	8.5 months
Project Managers	15%	19.75 months
Tech Support	10%	11.5 months

Breakdown of skills set for employees added to ecfirst management team 2007/2008 – sales and recruiting:

Skill set	% of skills placed
Business Analysts	30%
Project Managers	26%
QA Analyst	22%
Java, .Net, Architects	14%
Tech Support	8%

"Never be satisfied with what you achieve, because it all pales in comparison with what you are capable of doing in the future."

By Rabbi Nochem Kaplan

Management Team Biographies

Joanie Bond – New Business Account Manager

Joanie was an IT professional for 8 years with Principal working in PGI from 1995 to 1999 and Principal Bank from 1999 – 2002. Her roles varied from Developer, Network Support, Vendor manager, BA, QA and PM.

In 2003, Joanie ventured into IT Sales and worked with Principal from 2003 to 2005. In an 18 month period, she place **16** IT people at Principal performing solo for both the IT Sales and recruiter role. From 2005 – 2007, she opened a branch office for a Minneapolis firm to establish Wells Fargo account in a new, highly competitive market. In 21 months, she placed **58** IT people in the Des Moines market. Skill sets included desktop support, development, QA, BA, PM, Data Analysts and Architects.

Allen Nguyen – President and Founder of ecfirst

Allen has accrued over 18 years of intensive experience and has become an expert in Internet-enabling technology.

Prior to founding ecfirst, Mr. Nguyen spent a number of years consulting for several large corporations. In 1995, expecting to see a profound impact in the commercial arena, Allen co-founded ABC Virtual Communications, Inc. with the focus of helping companies to understand, embrace and implement Internet technology. With his help, the company grew from three to 60-plus employees in less than three years. During that time, he also helped build the company's technical infrastructure, led several enterprise-wide web development efforts, and was instrumental in developing and directing product development.

Some of Allen's technical achievements include the successful porting of Sun Microsystem JVM. His Java expertise also led him to design and implement the first 100% Java Applet application to automate the processing of forms from a web browser. Sun Microsystems, the inventor of Java, eventually licensed it for its own usage.

Allen remains actively involved in the day to day processes at ecfirst and actively screens technical consultants.

Contact Information:

Joanie Bond
Account Executive
515.453.8247 x22 office
515.314.8969 cell

Allen Nguyen
President and Founder
515.453.8247 x13 office
515.778.0024 cell

ecfirst.com

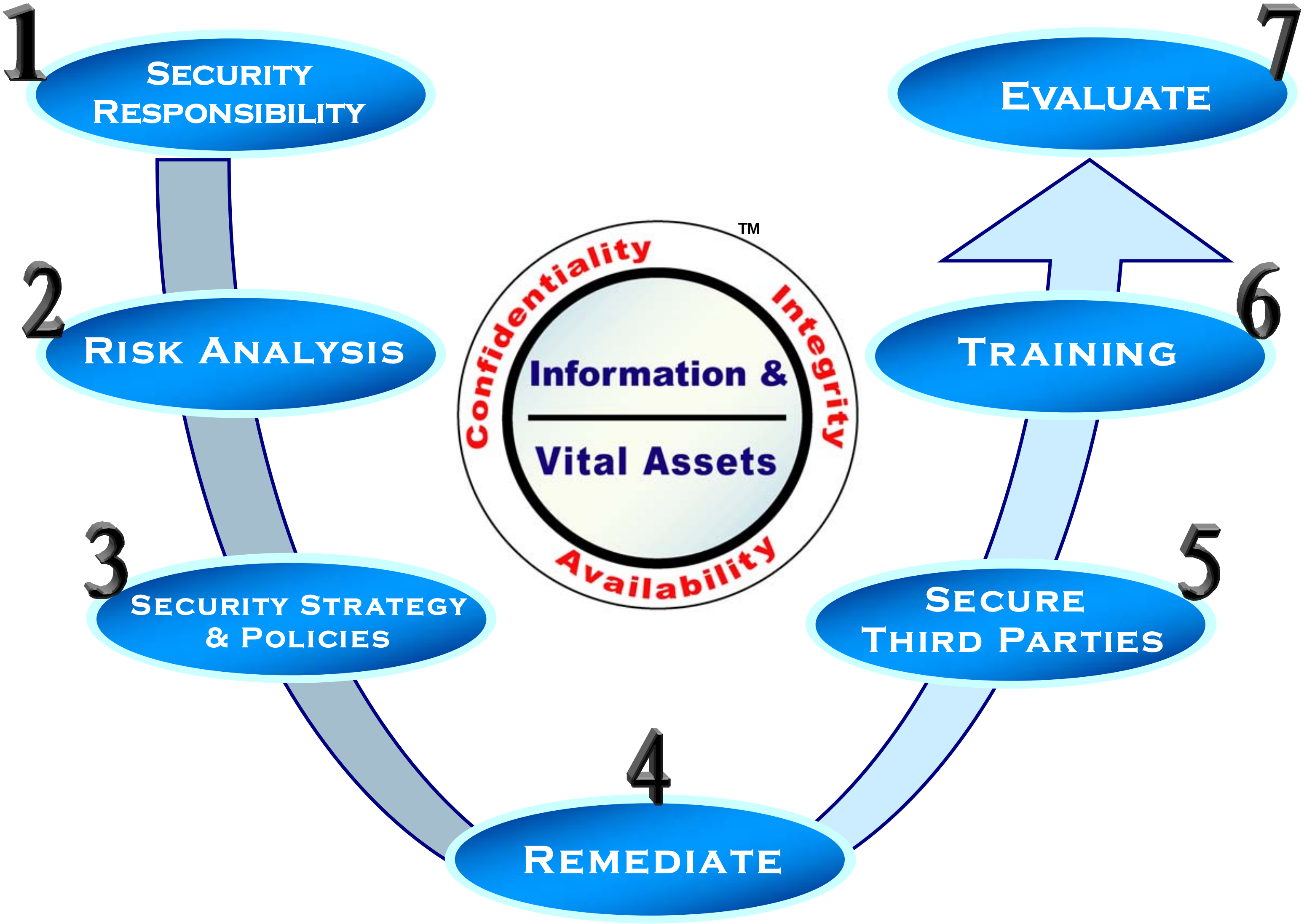
BizShield™

The Seven Steps to Enterprise Security™

ecfirst.com's **The Seven Steps to Enterprise Security™** is a Biz*Shield*™ methodology that establishes a comprehensive framework for defending your organization's sensitive information and vital assets. It is a road-map to safeguard not just your digital assets but the organization's information infrastructure as a whole. This methodology has been influenced by the domains defined in the **ISO 17799** and the **BS 7799** security standards as well as the **CobIT** and **NIST** security frameworks. It has also been impacted by the works of Sun Tzu's **Art of War** and India's legendary **Arthashastra** by Kautilya.

The **Seven Steps** methodology delivers *confidentiality, integrity and availability* (CIA) of your sensitive business information and other vital assets.

The **Seven Steps** methodology is **ecfirst.com's** road-map for securing your enterprise. It is the foundation of our Biz*Shield*™ Consulting Practice. Rich in hands-on security consulting experience, we are ready to address your enterprise security requirements.



www.ecfirst.com

877.899.9974 x20, x13 & x17

HIPAA Authentication: Proving Your Identity

Uday O. **Ali** Pabrai, S+, CHSS, SCNA – HIPAA Academy
Bob Tahmaseb, CISSP, CHSS – RSA Security, Inc.

The HIPAA Security Rule establishes and requires all health care organizations to meet its specifications for authentication and access control as defined in the Technical Safeguards category of the legislation. The focus of this article is on the HIPAA Security Rule requirements of person or entity authentication and access control and associated solution options for organizations to consider. We discuss the importance of strong authentication as a critical layer in establishing trusted digital identities. We then review several types of solutions to address the authentication requirement. These include Kerberos, digital certificates, authentication, tokens, smartcards and biometrics.

HIPAA Security Rule Authentication Requirements

The objective of the HIPAA Security Rule Person or Entity Authentication standard is to implement procedures to verify that a person or entity seeking access to electronic protected health information (e-PHI) is the one claimed. This is further emphasized in the Access Control standard, wherein the objective is to implement technical policies and procedures for electronic information systems that maintain e-PHI to allow access only to those persons or software programs that have been granted access rights as specified and such access must be based on a unique name and/or number for identifying and tracking user identity.   Simply put, organizations must have policies, procedures, and practices in place to uniquely identify users or resources accessing information.

Physical and Digital Identities

Authentication is about verifying the identity of an individual or an entity. Digital identification is a major challenge of all businesses. This is especially true for the health care industry where we need to confirm the identity of the individual or entity accessing e-PHI. Let us first define what we mean by an identity. For HIPAA purposes you have two identities. Your physical identity is you – your physical person, but you also have a "digital" identity as well. This digital identity is who you are in the digital world.

Glossary

Authentication: Is the ability to prove or validate the identity of a user or an entity.
Identification: Is the ability by which a user or entity provides a claimed identity to the system.
Authorization: Is the ability to control access to a resource. Access may be restricted on the basis of job role or function (rule).

Your physical identity will let you past the guard at the front desk with a photo badge and your digital identity determines what applications and online resources you have access to once you use a computer system. Your digital identity access may be based upon the position you have within an organization, a particular policy rule that may include you, or a group that you are a member of. The key to any digital identity is how you establish the link or trust with your physical identity. Tying your physical identity to your digital identity is accomplished with authentication.

The HIPAA Challenge

Conceptually, we must create an environment where only the right users access the right information. What HIPAA does not tell us is how we identify these users in order to give them access to the right information. This lack of detail is intentional. It is written to allow the owners of the information to use a broad range of methods to accomplish identification of users. First though, before we implement new solutions or evaluate existing practices, we must know what "identity" is as well as the various types of authentication available to us to prove identity.

What is "Identity"?

In the physical world we have ways of proving who we are. We can physically show a passport or drivers license that an authority has issued to us after verifying that we are who we say we are by examining something like a birth certificate. These credentials can now also be extended for use in proving your identity to other entities such as showing our drivers license at the grocery store when we write a check or using our passport at security checkpoints at the airport.This is identity. The core of identity is the ability to prove who you are via credentials and have those credentials accepted for use when trusted by other entities.

Establishing your identity in the digital world is a similar but harder process. We can not physically give a passport or drivers license to a networked resource to prove who we are. We can prove who we are by providing a form of authentication to tie our digital identity to our physical identity. Digital identity is established by the user by providing a unique name and a method of authentication when accessing a protected resource. An authority verifies who you say you are by this unique name and the level of trust associated with that user is established by the type of authentication method.

Types of Authentication

Not all authentication methods are equal. Some methods of authentication are considered stronger than others or the combining of different methods of authentication can be considered stronger than a single method alone. Authentication methods can be categorized into three different areas. These areas are something you know, something you have, or something you are. Each one of these areas has methods of authentication within them that are called form factors.

"Something You Know" (Knowledge)

Pins and passwords are the most common form factors of "something you know" authentication. Another "something you know" form factor could be an application or web page that requires you to enter answers to questions that you have previously answered when you enrolled. For example you may have to answer 5 of 7 questions correctly to gain access. A benefit of "something you know" type of authentication is that there is usually a low acquisition cost since most applications provide a password authentication method as part of the package at no extra charge. The downside is that "something you know" is often considered weak and easy to compromise. They are weak in that typically a pin or password consists usually a small word, number, or combination word/number that can be guessed or brute forced.

"Something You Have" (Possession)
The next form factor of authentication is "something you have". The most common of these include such things as smart cards, tokens, and digital certificates. Smart cards are a credit card sized pieces of plastic that have a processor imbedded in them. An authentication token is a device that generates a new value to be used for authentication each time it is accessed. These devices are small and are about the size of the remote control used to lock and unlock a car.

The last most common "something you have" form factors are digital certificates. A digital certificate is an envelope that contains information about you and your organization as well as a public and private key associated only with you. Digital certificates are most commonly used to provide encryption and digital signatures for email as well as by web servers to provide SSL sessions for encrypted Internet traffic. If you've ever bought anything online, you most likely presented your credit card information during an SSL encrypted session.

Each "something you have" form factors have varying cost, usability, storage, security and mobility issues associated with them. "Something you have" types of authentication are generally considered a stronger form of authentication than "something you know".

"Something You Are" (Person)
The last form factor of authentication is "something you are". This for the most part covers the use of biometrics to establish your identity. Biometrics relies on the unique individual nature of each of us to provide an identifying feature for authentication to a logical device such as a computer.

Strong Authentication

The strength of an authentication method is based on the number of factors it uses in verifying the identity of the entity. Strong authentication is where two or more authentication factors are used. You can combine multiple forms factors of authentication to more strongly prove your identity.

A common analogy for combining methods for authentication is your ATM card. An account holder does not go up to an ATM machine and enter just a pin or just insert their card to gain access to their money. They use both something they know; the pin, and something they have; the card, to do a two factor authentication to their account. For example, the most common form of two factor authentication is using a pin associated with a token. Many healthcare organizations are currently using or considering the use of two-factor token authentication to strongly identify and authenticate their users for access to e-PHI. You could also use a biometric device that is pin protected. Any way these form factors are mixed and matched the strength of the authentication relies using "something you know" with "something your have" or "something you are".

Recommendation

"Strong authentication, while not a HIPAA requirement, should be seriously considered for all administrative staff, such as system or network administrators and managers, that have access to sensitive business information such as e-PHI as well as those users that are accessing information remotely or externally from the organization"

Some organizations may even want, if the information being protected is considered extremely critical, to use three factor authentication. An example: a biometric template stored on a smart card that is pin protected. A user in this example would walk up to a computer, insert their smartcard, enter their pin, and place a finger on a biometric fingerprint reader to authenticate to a protected resource.

Implementation Criteria

The next step is deciding what authentication method to implement to identify your users. This can be a considerable task. It requires defining the sensitivity of the information, the routes the users are taking to access this information, and enablement technologies such as those that allow your users to authenticate once and gain access to multiple applications (commonly called Single Sign-on or SSO). Cost, resources, flexibility are just of few additional criteria for evaluating authentication methods.

Summary

Now you have a basic understanding of identity and authentication. Authentication helps identify you in the digital world. The type and strength of that authentication helps owners of information establish that you are who you say you are. The stronger the authentication method used, the more an owner of information can trust a user attempting to access that information.

Author Bio

Uday O. **Ali** Pabrai is the creator of the first program on HIPAA skills certification and author of the #1 book on HIPAA, *Getting Started with HIPAA*, Ali's clients have included Blue Cross Blue Shield Affiliates, several state and county governments, Wells Fargo, U.S. Defense Intelligence Agency, U.S. Naval Surface Warfare Center, FDLE, Microsoft, CBOE, Kemin Industries, Marsh and many others. Ali may be reached at Pabrai@HIPAAAcademy.Net.

Bob Tahmaseb has been many things including an Army Intelligence Officer, Department of Defense Security Manager, and a White Hat Hacker. He currently is a Principal Systems Engineer with RSA Security, Inc. As an engineer for RSA he helps provide many organizations with authentication, identity & access management, and digital certificate solutions. Bob holds the Certified Information Systems Security Professional, RSA Certified Systems Engineer, Certified HIPAA Professional and Certified HIPAA Security Specialist certifications. Bob may be reached at btahmaseb@rsasecurity.com

For internal use only. Not for distribution.

Secure Your Wireless Infrastructure

When you deploy wireless technology components, you must follow policy requirements to ensure consistency and security, and address other critical elements to secure confidential business information.

BY UDAY ALI PABRAI, CISSP, CHSS, ECFIRST.COM CHIEF EXECUTIVE

EXECUTIVE SUMMARY

Wireless network security isn't the same to implement as the wired variety. Companies face many challenges to overcome while realizing the benefits of a wireless network. The transfer of highly sensitive patient information in particular must be handled with care. Here's what to consider for your wireless network policy.

Companies in all industries are deploying wireless networks. In some instances, these deployments have resulted in terrific efficiencies. For example, in the healthcare industry, nurses traditionally record information on paper about patient vitals at hospitals or long term care facilities. Today, several companies are deploying personal digital assistants (PDAs) with wireless capability to support the real-time transmission of vital information stored about patients — right at the point of care location. This article discusses the challenges companies face when implementing a secure wireless infrastructure.

Gartner reports that through 2006, 70 percent of successful wireless local area network (WLAN) attacks will occur because of misconfigured access points or client software. Security professionals base security for today's businesses for the most part on protocols and technologies that support a wired infrastructure. The proliferation of mobile devices and wireless communication is introducing new security gaps businesses must address. As the saying goes, security is only as good as your weakest link, and wireless systems are the weak links in business infrastructure. Security and compliance practitioners need to better understand wireless technologies, protocols, and standards and develop a policy to address wireless security to ensure these technologies are not the "gaps" exploited by hackers.

HIPAA COMPLIANCE SECURITY REQUIREMENTS

Table 1 identifies the Health Insurance Portability and Accountability Act (HIPAA) implementation specifications in the Technical Safeguards section of the HIPAA Security Rule. The requirements related to Access Control, Audit Control, Person, or Entity Authentication and of course, Transmission Security are all significant as you identify safeguards and controls to secure wireless devices and their transmission on your digital information infrastructure.

WIRELESS NETWORK STANDARDS

A working group at the Institute of Electrical and Electronics Engineers (IEEE) defined the 802.11 standards for wireless networks. These wireless networks are basically Ethernet networks without cables. Here is a summary of the IEEE 802 wireless standards:

- 802.1x is a framework for stronger authentication for 802.11 WLANs.
- 802.11ais a physical layer standard in the 5GHz radio band. Maximum link rate is 54Mbps per channel.
- 802.11b is a physical layer standard in the 2.4GHz radio band. Maximum link rate is 11Mbps per channel.
- 802.11d is supplementary to MAC layer in 802.11. Supports use of 802.11 WLANs.
- 802.11e provides QOS and multi-media capability.

Continued

Uday Ali Pabrai, Security, CISSP, CHSS, chief executive of ecfirst.com, consults extensively in the areas of enterprise security and regulatory compliance (http://www.HIPAAacademy.Net). He is the author of *The Art of Information Security*, and is the creator of HIPAA and security certification programs. Uday's clients have included the U.S. Naval Surface Warfare Center, Microsoft, U.S. DIA, Wells Fargo, Kemin, Elkay, Marsh, and many others. ecfirst.com is an Inc. 500 organization. Pabrai@ecfirst.com

Table 1: Technical Safeguards in the HIPAA Security Rule — Follow these to identify what you need to secure wireless devices and transmissions.

Standards	Implementation Specifications	R = Required
		A = Addressable

Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	R
Audit Controls		R
Integrity	Mechanism to Authenticate Electronic PHI	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

- 802.11f defines the registration of access points within a network and exchange of information between access points when a user is handed over from one access point to another.
- 802.11g is a physical layer standard for WLANs in the 2.4GHz and 5GHz radio band. Maximum link rate is 54Mbps per channel.
- 802.11h is supplementary to MAC layer to comply with EU regulations for 5GHz WLANs.
- 802.11i is supplementary to MAC layer to improve security. Alternative to WEP with new encryption methods and authentication procedures.
- 802.16a extends the range of 802.11 to several miles. Provides enhanced security and supports high quality phone calls.
- 802.20 extends the range of 802.11 to several miles and is being designed to support high-speed links in cars and trains traveling at speeds exceeding 120 miles per hour.

WIRELESS NETWORK COMPONENTS

IEEE 802.11wireless LANs include the following components:

- Wireless Network Interface Card, which may be PC, USB, or PCI cards that interfaces between the client computer and the communications medium. It converts digital data to and from radio waves.
- Client System may be a laptop, PDA, or a desktop system.
- Communications Medium consists of radio waves in the 2.4GHz or 5GHz radio frequency band. The frequency band is broken up into channels.
- Access Point is a hardware device that provides several channels to connect client systems to the wired LAN.

The components may be connected in one of two types of operating modes. The IEEE 802.11 standard defines two specific operating modes:

- Ad-Hoc
- Infrastructure

In the Ad-Hoc mode, two or more client systems create a peer-to-peer network with each other's wireless NICs through a mesh network. This network is typically formed on a temporary basis.

In the Infrastructure mode, client systems connect to an access point. The access point is connected to the wired network. Client systems communicate with each other through the access point.

Before a client system can connect to an access point, the system must provide a Service Set Identifier (SSID) that identifies the wireless network. The SSID is an alphanumeric code that's configured on the wireless network interface card (NIC) and the access point. SSIDs provide a configurable identification that lets wirless clients communicate with the appropriate access point.

WIRELESS SECURITY CHALLENGES

Lack of user authentication, weak encryption, and poor network address management are some examples of security challenges of wireless networks. For example, an access point can authenticate hardware based on MAC or IP addresses and not require user authentication. Further, although you can use the wired equivalent protocol (WEP) to encrypt wireless transmission, the encryption is weak and easy for hackers to break. Hackers can also monitor unencrypted transmissions to determine SSIDs. SSIDs provide information on the name and availability of a wireless network.

Wireless networks are also vulnerable to attacks, such as:

- Rogue access points ("Man-in-the-middle")
- Session hijacking
- Denial of Service

Here's more on each of these types of attack.

In a wireless infrastructure, the access point is an interface between the wireless network and a wired network that authenticates the client and authorizes the connection. The client doesn't authenticate the access point. It's thus possible for an attacker to set up a rogue access point with the same SSID and a stronger signal; this rogue access point then "traps" all information from the client to the authorized access point. It essentially is an example of a "man-in-the-middle" attack. The client doesn't know the rogue access point is receiving the communication.

Another example of an attack is session hijacking. Here the attacker sends a "dissociation" message to the client, dropping the client from the connection to the access point. The attacker then spoofs the access point with identification information of the client and continues the communication.

In a denial of service attack, the attacker emulates the access point and continuously sends de-authentication and disassociation messages to the client systems. The clients are unable to connect to the access point and aren't able to establish a connection. The attacker can also jam radio signals by generating enough radio noise in the frequency range used. This again prevents clients and access points from communicating.

WIRELESS SECURITY PROTOCOLS

The IEEE has defined several standards and protocols to better secure wireless networks. These include:

Continued

- Wired Equivalent Privacy (WEP)
- IEEE 802.1x User Authentication
- Extensible Authentication Protocol (EAP)
- Lightweight Extensible Authentication Protocol (LEAP)
- Wi-Fi Protected Access (WPA) and WPAv2

Let's take a closer look at each of these wireless security-related specifications.

Wired Equivalent Privacy (WEP) is the standard 802.11 wireless security protocol for data encryption. It uses a key to encrypt wireless data transmitted through the radio waves. It supports a 40-bit key and a 128-bit key. Attackers have been able to compromise both WEP key lengths.

IEEE 802.1x User Authentication: 802.1x is an IEEE standard that works with WEP to provide the framework for strong authentication. The IEEE 802.1x consists of three components:

1. Supplicant: The client system trying to access the wireless network
2. Authenticator: Provides the physical port to the network, such as an access point or a switch
3. Authentication Server: Verifies user credentials and provides key management; may be a RADIUS server, LDAP directory, Windows NT Domain, or an Active Directory

Extensible Authentication Protocol (EAP) is an authentication protocol 802.1x components use to let users authenticate to a central server. After the server authenticates the client, keys are sent to both the authenticator (the access point) and the supplicant (the client).

Lightweight Extensible Authentication Protocol (LEAP): Cisco developed LEAP; it is also referred to as the Cisco Wireless EAP.

Wi-Fi Protected Access (WPA), WPAv2, and IEEE 802.11I: Wi-Fi Protected Access (WPA) is the standard in wireless security to address the weaknesses in the WEP algorithms. WPA addresses two areas of security: authentication and encryption. It combines the 802.1x authentication with a stronger encryption. The encryption is based on the IEEE 802.11i standard, referred to as the Temporal Key Integrity Protocol (TKIP). Note that the 802.11i standard, also referred to as WPAv2, includes the specification Counter Mode with CBC-MAC Protocol (CCMP). CCMP uses the Advanced Encryption Standard (AES), thus providing very strong encryption capability. Certified by the W-Fi Alliance, WPAv2 products are backward compatible with WPA-certified products. Both WPA and WPAv2 use 802.1x and EAP for authentication. WPAv2 encryption is based on the advanced AES standard.

GETTING STARTED WITH A WIRELESS SECURITY POLICY

Security practitioners should develop a policy for securing wireless devices and transmissions. The scope of this policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the company's networks, including any form of wireless communication device capable of transmitting packet data.

This policy should include specific recommendations, such as:

- Wireless implementations must maintain point-to-point hardware encryption of at least 128 bits.
- Wireless devices must maintain a hardware address that can be registered and tracked, i.e., a MAC address.
- Wireless devices must support strong user authentication that checks against an external database such as TACACS+, RADIUS or something similar.
- Laptop/PDA users should select strong passwords and must have anti-virus software installed with automatic updates.
- Screen savers must be activated if a computer is idle for two to three minutes.
- Laptop users must use encryption to store sensitive information on laptops.
- Wireless design should be done using best practices

The core objective in the design of the wireless network must be to minimize the number of access points, because each represents a potential point of vulnerability. Further, you must install (or, "companies must install") the access points away from exterior walls so the strength of the signal is reduced for access from outside the physical facility. You shouldn't install the access point on the same network as other network resources. The key here is to understand the risk to the infrastructure if the access point is compromised. It should typically be separated from the wired network and the design should require communication to go through a firewall system.

Base your enterprise wireless infrastructure upon these guidelines:

- Configure a firewall between the wireless network and the wired infrastructure.
- Ensure that 128-bit or higher encryption is used for all wireless communication.
- Fully test and deploy software patches and updates on a regular basis.
- Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.

Base your access points configuration upon these guiding principles:

- Maintain and update an inventory of all access points (AP) and wireless devices.
- Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
- Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- Change the default settings on APs, such as those for SSIDs.
- Restore APs to the latest security settings when the reset functions are used.
- Ensure all APs have strong administrative passwords.
- Enable user authentication mechanisms for the management interfaces of the AP.
- Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
- Turn on audit capabilities on AP; review log files on a regular basis.

Configure all mobile devices, such as PDAs and laptops that have wireless capability to support:

- Installing anti-virus software on all wireless clients.
- Installing personal firewall software on all wireless clients.
- Disabling file sharing between wireless clients.

MINIMIZE YOUR RISKS

Sensitive and confidential information transmitted over wireless networks is typically not encrypted and lacks proper authentication. A vulnerable wireless infrastructure is a significant risk to business. It exposes the company's sensitive information to legal liabilities, compliance violations, and more. Security practitioners must understand wireless technologies and standards and create a security policy that addresses risks associated with a wireless infrastructure. When you deploy wireless technology components, follow policy requirements to ensure consistency and security. You must address the critical elements of user authentication as well as encryption to secure confidential business information.

Review the design of the perimeter to address wireless entry and exit points between internal and external (Internet) networks. Educate users on wireless policies so they will use their mobile devices securely to access the network. The bottom line is this: Don't make your wireless infrastructure the weak link in your digital information ecosystem. ADVISOR

DATA MANAGEMENT • SHOULD YOU OUTSOURCE DATA STORAGE?

Continued from page 20

data storage needs — from back-ups to e-mail archiving — without risking data security. Before outsourcing data to a third-party storage provider, consider the following questions:

- What sensitive data are you sending to the third-party provider? Will you include customer data protected by privacy laws?
- Who can access the data? Can the service provider's staff access the content of your data? Could anybody intercept it in transit?
- What processes and procedures are in place to ensure data is secure and protected from unauthorized access?

WHAT TO LOOK FOR IN AN OUTSOURCED SOLUTION

Keeping these questions in mind, companies should look for key attributes — ranging from encryption to round-the-clock support — in a service provider before outsourcing their data storage.

Encryption

Data encryption is a critical step in securing data for storage. According to recent recommendations by Gartner, a research/analyst firm, companies should use encryption as the primary security technology for backup storage of all sensitive data. Encryption not only protects data in accordance with the SB 1386 data privacy law (when data is encrypted, companies aren't required to report stolen or lost data), it also reduces the likelihood of a security breach in the first place (internal staff or other people with knowledge of what the data contains conduct a high percentage of data breaches). In addition, encrypting can save a company the millions of dollars it costs to recover from data theft or loss.

Although encryption of data during transit is becoming more common, the encryption of data at rest — data stored in company databases — isn't as prevalent. To prevent an outsourcer's employees from accessing the content of data, you should consider encrypting stored data. In the past, this feature made searching through data difficult or impossible but new technologies have overcome this barrier.

In fact, some outsourcers now offer services that keep data encrypted at all times after it leaves the corporate firewall. You can implement this encryption by placing an appliance at the customer site, which encrypts the data and maintains the encryption keys. Only someone with access to both the appliance and the data network can search or retrieve data. This hybrid approach will likely become more common among service providers as customers continue to demand greater levels of security.

Infrastructure security

When you outsource your data storage, you should protect the physical and network infrastructure with multiple levels of security. In many cases, companies place servers in geographically diverse datacenters, and you should also engineer them for maximum security using such measures as: round-the-clock security guards, video surveillance, and electronic security systems that control access to the datacenter.

24 x 7 x 365 support

Outsourcing your data requires total support, regardless of the day or time. It's incredibly important to ensure the outsourcer you choose has the right people behind their technology to help you if things don't work as promised. Always look for a technical support team that's available 24 x 7.

LOOK FOR A SPECIALIST

When outsourcing your data storage, you should look for a specialized vendor. Consider whether storage makes up the company's core business, or if it's only one of many services offered. When data storage is a core service, providers will more likely fully commit to keeping data secure and staying in touch with evolving challenges such as regulatory compliance and legal discovery. After all, one of the benefits of outsourcing is gaining expertise that might not exist in-house. A high level of expertise should be a primary requirement.

With the right security controls in place, the benefits of outsourcing can easily outweigh the disadvantages, making it a valuable option for any company looking for better ways to manage and store its ever-growing mass of data. ADVISOR ecfirst.com HEALTHCARE

BizShield™

Managed Compliance Services for HIPAA

Meeting the Recurring Regulatory Requirements of the Health Insurance Portability and Accountability Act - Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) regulates the privacy and security of personal health information. HIPAA refers to this information as Protected Health Information (PHI). The legislation mandates healthcare organizations to maintain compliance with reasonable and appropriate safeguards in several specific areas. **On a regular schedule, healthcare organizations must:**

- Conduct a comprehensive and thorough risk analysis
- Complete a Business Impact Analysis (BIA) for contingency planning and disaster recovery
- Develop and update security policies and procedures
- Train members of the workforce
- Audit and evaluate the information infrastructure

The information infrastructure within healthcare organizations is constantly changing, and new systems such as clinical, financial or others are adding to the complexity. Compliance must be maintained as changes are introduced. Further, attacks on the infrastructure are a 24x7 activity and the volume of personal health information flowing within the organization is increasing at an unprecedented pace. This is causing significant resource strains on the existing IT staff and management. Also, in most environments, the specialized skills required and typical of credentialed professionals in IT are lacking within the healthcare organization.

ecfirst.com Healthcare's **Managed Compliance Services** are tailored to meet HIPAA's requirements and provide you with specialized capability in the areas of vulnerability assessments, BIA and contingency planning, training and certification, as well as audit and evaluation. We focus on regulatory requirements and keeping you compliant, so you can focus on your business of delivering exceptional patient care and services.

The benefits of outsourcing HIPAA compliance include minimizing productivity losses from unexpected downtime, enabling staff to better focus on business-critical tasks and complying with key regulations within HIPAA. Also, Managed Compliance Services provides you with further depth in resource capabilities with trusted knowledge of your infrastructure. This can help smooth out volatility in resource demands and costs associated with managing information technology.

Table 1 specifically identifies HIPAA requirements addressed by Managed Compliance Services.

HIPAA Regulation	**HIPAA Requirement**	**Managed Compliance Service**
Risk Analysis 164.308(a)(1)	Conduct an accurate and thorough assessment of the potential risks to and vulnerabilities of the confidentiality, integrity and availability of the entity's electronic protected health information (EPHI).	On an annual basis we will conduct a thorough security vulnerability assessment followed by a comprehensive Risk Assessment highlighting the gaps and providing recommendations for remediation.
Assigned Security Responsibility 164.308(a)(2)	Covered entities must identify the security official who is responsible for the development and implementation of the Security Rule's required policies and procedures.	An interim security officer will be assigned to your organization to meet compliance requirements. Service is flexible and can be tailored to a few hours a week to a full-time on-site staff position.
Security Awareness and Training 164.308(a)(5)	Covered entities must implement a security awareness and training program for all members of the workforce.	On-line content will be provided for on-going training for HIPAA Security for all members of the workforce. Content can easily be tailored based on job role requirements defined by your organization. Limited number of IT professionals and managers will be provided with vouchers to attend the 4-day HIPAA certification program delivered nationally. On an annual basis, we will conduct an executive briefing for senior management covering topics like industry best practices, advancements in information security technologies and changes in legislation & accreditation standards.
Contingency Plan 164.308(a)(7)	Covered entities must establish policies and procedures for responding to an emergency.	On an annual basis we will conduct a business impact analysis and provide recommendations for Business Continuity / Disaster Recover planning.
Evaluation 164.308(a)(8)	Covered entities must perform periodic evaluations to determine the extent to which the security policies and procedures meet the Rule's requirements.	On an annual basis we will evaluate the organization's policies and procedures to meet compliance requirements. Policies will be updated as required.

Table 1: HIPAA Requirements and Managed Compliance Services.

Hospitals Trust the American Hospital Association (AHA)

And the American Hospital Association (AHA) has exclusively endorsed ecfirst.com's HIPAA training and certification programs. Every business day we are delivering HIPAA solutions, both training and consulting, to hospitals across the United States. Our organization introduced the first program in the industry to comprehensively cover the HIPAA regulation. Our HIPAA training and certification programs have been attended by hundreds of organizations and thousands of professionals. Our clients include the U.S. Army, U.S. Air Force, U.S. Coast Guard, U.S. Department of Homeland Security, many state and county governments and hundreds of hospitals, long term care, assisted living and other organizations.

Hospitals Trust ecfirst.com Healthcare

Why trust managed services from ecfirst.com Healthcare? Because when we deliver services, we bring not just a technology solution, but an in-depth understanding of hospitals as well as deep knowledge of compliance requirements. We believe that business and technology challenges need to be aligned to achieve success with projects and initiatives on a continual basis. We only include credentialed, experienced professionals in our engagements.

ecfirst.com Healthcare Clients

Edward Hospital and Health Services
Samaritan Hospital
BSA Hospital
Condell Health Network
Passavant Hospital
St. Anthony's Hospital
Northwest Community Hospital
The Children's Hospital of Philadelphia
North Broward Hospital District
Shriners Hospitals for Children, Chicago
RML Specialty Hospital
Rockford Health System
Shriners Hospital for Children
CGH Medical Center
Richland Memorial Hospital
IPMR
Tufts-New England Medical Center

Provena Health
U of I Medical Center
Memorial Hospital
Washington County Hospital
Hammond-Henry Hospital
Hospital Perea
Siskin Hospital for Physical Rehabilitation
Mercy Medical Center
Madigan Army Medical Center
Memorial Healthcare System
Sarah D. Culbertson Memorial Hospital
Alameda County Medical Center
Picken County Medical Center
Native American Health Center, Inc.
Children's Hospital & Research Center at Oakland

Investment (for 200-500 bed hospital)

HIPAA Regulation	**Managed Compliance Service**	**Estimated effort**	**Price/year**
Risk Analysis 164.308(a)(1)	On an annual basis we will conduct a thorough security vulnerability assessment followed by a comprehensive Risk Assessment highlighting the gaps and providing recommendations for remediation.	45 days	$45,000
Assigned Security Responsibility 164.308(a)(2)	An interim security officer will be assigned to your organization to meet compliance requirements. Service is flexible and can be tailored to a few hours a week to a full-time on-site staff position.	25 days	$25,000
Security Awareness and Training 164.308(a)(5)	On-line content will be provided for on-going training for HIPAA Security for all members of the workforce. Content can easily be tailored based on job role requirements defined by your organization. Limited number of IT professionals and managers will be provided with vouchers to attend the 4-day HIPAA certification program delivered nationally. On an annual basis, we will conduct an executive briefing for senior management covering topics like industry best practices, advancements in information security technologies and changes in legislation & accreditation standards.	Content 2 seats 1 day	$7,500 $5,000 Free
Contingency Plan 164.308(a)(7)	On an annual basis we will conduct a business impact analysis and provide recommendations for Business Continuity / Disaster Recover planning.	60 days	$60,000
Evaluation 164.308(a)(8)	On an annual basis we will evaluate the organization's policies and procedures to meet compliance requirements. Policies will be updated as required.	20 days	$20,000
	Total		$162,500
	Total if a three year contract is signed (at 20% discount)		$130,000
	Amount to be paid per month		**$10,833**

About ecfirst.com Healthcare

ecfirst.com is a leader with rich hands-on experience delivering world-class services in the areas of:

- Security regulatory compliance solutions (HIPAA, FISMA, Sarbanes-Oxley)
- Compliance training and certification
- Service Oriented Architecture (SOA) consulting and development
- Professional staffing, including project management

Regulatory Compliance Practice
The ecfirst.com Regulatory Compliance Practice delivers deep expertise with its full suite of services that include contingency planning/Business Impact Analysis (BIA), secure single sign-on, vulnerability assessment, as well as managed security and IT infrastructure solutions.

Compliance and Training certification
ecfirst.com, home of the HIPAA Academy, offers the gold standard in compliance training and is endorsed by the American Hospital Association (AHA). The HIPAA CHA^{TM}, CHP and CHSS^{TM} certifications are the only certifications recognized in the Industry.

Credentialed Professional Staffing Practice
The ecfirst.com Professional Staffing Practice excels in meeting your short and long term requirements for contract professionals in the areas of Web development, IT and project management. This practice is distinguished with credentialed staff (PMP, CBCP, CISSP, CSCS or CHSS) that includes deep industry knowledge in the healthcare, financial and government markets.

ecfirst.com assists all types of organizations with their compliance initiatives for a secure information infrastructure that is compliant with regulation requirements. ecfirst.com can help you with your compliance challenges and priorities. ecfirst.com solutions help your organization implement the security safeguards required as a result of the legislation requirements.

ecfirst.com, an Inc. 500 business, serves a Who's Who client list that includes Wells Fargo, U.S. Veterans Agency, numerous hospitals, state and county governments (State of Oregon, Iowa,, Illinois), and hundreds of other organizations.

ecfirst.com is endorsed by the American Hospital Association (AHA) and the Illinois Hospital Association (IHA).

We understand that if, and only if, we deliver exceptional value to your organization in every instance of our engagement, will we be able to have you as a customer for life. All our work is executed with deep knowledge of your industry and compliance requirements by quality staff with certifications that substantiate their expertise. We are always striving to earn your trust.

Ask for a free copy of *The Art of Information Security* (limited to one per organization only). For more information, please visit http://www.ecfirst.com.

Contingency Planning for HIPAA: Are You Ready for the Unexpected?

Planning, documenting, testing, and communicating are all areas you should address comprehensively and thoroughly to position the business to continue to deliver services.

BY UDAY ALI PABRAI, CISSP, CHSS, ECFIRST.COM CEO

EXECUTIVE SUMMARY

Companies are adopting ORM to help them meet corporate governance regulations, identify and manage risk beyond financial reporting, and maximize business performance. This article explains more about the ORM adoption phases and how ORM relates to compliance issues.

Of the more than US$40 billion insurance companies paid out because of the September 11 attacks, more than 25 percent — $11 billion — was for claims related to business interruption. Some industry experts say that among companies that suffer significant, sustained disasters, 20 percent are completely out of business within 24 months. Yet most health care companies today don't have contingency plans. Contingency plans are a federal requirement for health care companies and a key part of the HIPAA Security Rule. For many of those that do have plans, those plans are often out of date or ignore key human factors; worse yet, many plans are untested. Why should security professionals and officers care about contingency planning? Because contingency plans address the "availability" security principle. The availability principle addresses threats related to business disruption, so authorized individuals have access to vital systems and information when required.

CONTINGENCY PLAN DEFINED

Contingency planning, also referred to as Business Continuity Planning (BCP), is a coordinated strategy that involves plans, procedures, and technical measures to enable the recovery of systems, operations, and data after a disruption.

Companies must develop the contingency plan with the input and support of line-of-business managers and all key constituencies, because the plan will need to work across the company. Businesses must base the plan on the risks faced by the company as well as risks associated with partners, suppliers, and customers. All technology issues must be addressed in the context of business operations. Businesses must regularly test and refine the plan itself as required.

The core objectives of contingency planning include the capability to:

- Restore operations at an alternate site (if necessary)
- Recover operations using alternate equipment (if necessary)
- Perform some or all of the affected business processes using other means

BUSINESS IMPACT ANALYSIS (BIA)

One of the critical steps in contingency planning is BIA. BIA helps to identify and prioritize critical Information Technology (IT) systems and components. IT systems may have numerous components, interfaces and processes. BIA enables a complete characterization of:

- System requirements
- Processes
- Interdependencies

As part of the BIA process, businesses collect, analyze, and interpret information. The information provides the basis for defining contingency requirements and priorities.

The objective is to understand the impact of a threat on the business. The impact of the threat

Uday Ali Pabrai, Security, CISSP, CHSS, Chief Executive of ecfirst.com, consults extensively in the areas of enterprise security and regulatory compliance (http://www.HIPAAacademy.Net). He is the author of The Art of Information Security, and is the creator of HIPAA and security certification programs. Uday's clients have included the U.S. Naval Surface Warfare Center, Microsoft, U.S. DIA, Wells Fargo, Kemin, Elkay, Marsh, and many others. ecfirst.com is an Inc. 500 organization. Pabrai@ecfirst.com

may be economical, operational, or both. Questionnaires or survey tools may be used to collect the information.

CLASSIFICATION OF INFORMATION

It might be necessary for companies to prioritize their sensitive business information into categories. An example of this is what was done by the Massachusetts Institute of Technology in its Disaster Recovery and Business Resumption Plans. Their categories were:

- Category I, Critical: Must be restored to maintain normal processing
- Category II, Essential: Will be restored as soon as resources become available, not to exceed 30 days
- Category III, Necessary: Will be restored as soon as normal processing is restored, data must be captured and saved for subsequent processing
- Category IV, Desirable: Will be suspended for the duration of the emergency

CLASSIFICATION OF THREATS

The National Institute of Standards and Technology (NIST) has identified three classifications of threats:

1. Natural — hurricane, tornado, flood, and fire
2. Human — operator error, sabotage, implant of malicious code, and terrorist attacks
3. Environmental — equipment failure, software error, telecommunications network outage, and electric power failure

Systems are vulnerable to a variety of disruptions, ranging from mild, such as short-term power outage or a disk drive failure to severe, such as equipment destruction and fire. Businesses can minimize or eliminate many vulnerabilities through technical, management, or operational solutions as part of the company's risk management effort; however, it's virtually impossible to completely eliminate all risks. Contingency planning is designed to mitigate the risk of system and service unavailability by focusing effective and efficient recovery solutions.

CONTINGENCY PLAN COMPONENTS

Every business must develop a contingency plan. Typically, the contingency planning coordinator is responsible for the contingency planning process. This individual may be the security officer or CIO, or an individual with management responsibilities and experience in this area. The company should formally identify this person and the team that will be working closely together to develop the contingency plan.

The HIPAA Security Rule identifies specific requirements to address the area of business continuity. The contingency plan document must specifically address the following critical components:

- Data Backup Plan (Administrative safeguard)
- Disaster Recovery Plan (Administrative safeguard)
- Emergency Mode Operation Plan (Administrative safeguard)
- Testing and Revision Procedure (Administrative safeguard)
- Applications and Data Criticality Analysis (Administrative safeguard)
- Contingency Operations (Physical safeguard)
- Physical Security (Physical safeguard)
- Data Backup and Storage (Physical safeguard)
- Emergency Access Procedures (Technical safeguard)

The data backup plan is a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information. Successful data backup and restores are sometimes dependent upon business processes and "batch" activities. The company needs to carefully test all critical backups and restores on a schedule related to the criticality of data to the company.

A disaster recovery plan provides a blueprint to continue business operations in the event a catastrophe occurs. The disaster recovery plan must include contingencies for the period of time of the disaster and until the recovery plan can be completely implemented.

An emergency mode operation plan is the part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure. Companies must consider identifying the levels of emergencies and associated responses.

Testing and revision procedures are for processing of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary. These written testing and feedback mechanisms are the key to successful testing. The tests conducted may be walk-throughs or document reviews, simulation test or checklist testing, or may very well be a full interruption test to test all aspects of the contingency plan.

Applications and data criticality analysis lets businesses assess the relative criticality of specific applications and data in support of other contingency plan components. It is an entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits. This procedure begins with an application and data inventory.

Contingency operations establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operation plan in the event of an emergency.

Physical security is a critical aspect of disaster and business continuity planning. Administrative controls for physical access to enable contingency operations must be in place so recovery can proceed as defined in plans.

Data backup and storage on a continual and consistent basis are required as one cannot be sure when a company may experience some disaster that will require access to backed up data and need it to be back in operation. Data may also be lost or corrupted; hence a good data backup plan is important. Data backup methods include full, incremental or differential. Data backup and storage addresses questions such as:

- Where will the media be stored?
- What is the media labeling scheme?

Continued on page 19

started planning operational risk programs. For instance, many have one-off initiatives underway, implementing operational risk activities around financial reporting initiatives as driven by Section 404 SOX requirements. A key trademark of a Phase 2 organization includes newly formed committees with representatives from Audit, Finance, IT, Physical Security, HR, and Information Security dedicated to managing risk to business activities.

Phase 3: Implementation

A growing number of enterprises (particularly in the financial services, healthcare, government, and energy vertical industries) have set up more formal ORM frameworks and have designated resources for operational risk (e.g., creation of the role of chief risk officer). Enterprises within this category have several risk management initiatives underway and have started to identify and measure basic operational risk indicators. They have also begun to invest in risk management tools to begin to analyze, mitigate, and, ultimately, manage issues and incidents before they become losses.

Phase 4: ORM Nirvana

A few enterprises have entered Phase 4. This phase uses a holistic, enterprise-wide approach where anyone can input and access data throughout the organization, from senior management out to the business line owners and operators, and conduct various types of analyses to maximize the efficiency of the business and reduce the cost of operational risk and loss.

MITIGATE RISK AND INCREASE PERFORMANCE

Regardless of the ORM phase in which organizations find themselves, SOX and other corporate governance regulations are here to stay. Risk is inherent in all organizations. To meet these corporate governance regulations, an enterprise must implement a framework for identifying and managing risk beyond financial reporting. Not only can they mitigate this risk by implementing ORM, but they can also maximize business performance throughout the organization. The ORM vision is to create an environment where all personnel manage operational risk, and all strategic objectives are completed at the least possible cost to the organization.

HIPAA

Continued from page 15

- How quickly will data need to be recovered in the event of an emergency?
- How long will data be retained?
- What is the appropriate media type used for backup?

Emergency access procedures are implemented as needed for obtaining necessary sensitive business information during an emergency. Emergency access is a necessary part of access control and will be necessary under emergency conditions, although these may be very different from those used in normal operational circumstances. For example, in a situation where normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed sensitive information.

TYPES OF BACKUP SITES

Businesses may consider several options for a backup site to address specific contingency plan requirements. The options for types of backup sites include:

- Cold sites
- Warm sites
- Hot sites
- Mobile sites
- Mirrored sites

A cold site is a facility with adequate space and infrastructure to support the IT system. The site does not include the IT systems, but does provide the infrastructure for the systems. A warm site includes some office spaces and some or all of the system hardware and software components. A warm site is maintained in an operational status to receive the relocated system.

A hot site is typically staffed 24 X 7 and supports all system requirements, supporting infrastructure as well as support personnel. A mobile site is a self-contained transportable environment that includes the required telecommunications and other IT equipment to meet contingency requirements. A mirrored site has fully redundant facilities and supports real-time information mirroring. A mirrored site is identical to the primary site in all technical areas.

A cold site is the least expensive while a mirrored site is the most expensive.

TOP PRIORITY

A 2005 Global Information Security Survey identified disaster recovery/business continuity as a top strategic priority for companies in their "to-do" list. Gartner reports that around two out of five companies experiencing some sort of disaster actually go out of business within five years of the incident. Planning, documenting, testing, and communicating are all areas to address comprehensively and thoroughly to position the business to continue to deliver services. Further, several regulatory legislations require companies to specifically develop a contingency plan. Security practitioners and the officer must work closely with the contingency team to ensure the plan addresses security requirements for supporting continuity of critical business functions in the event of a disaster.

HIPAA ACADEMY™

Regulatory Compliance

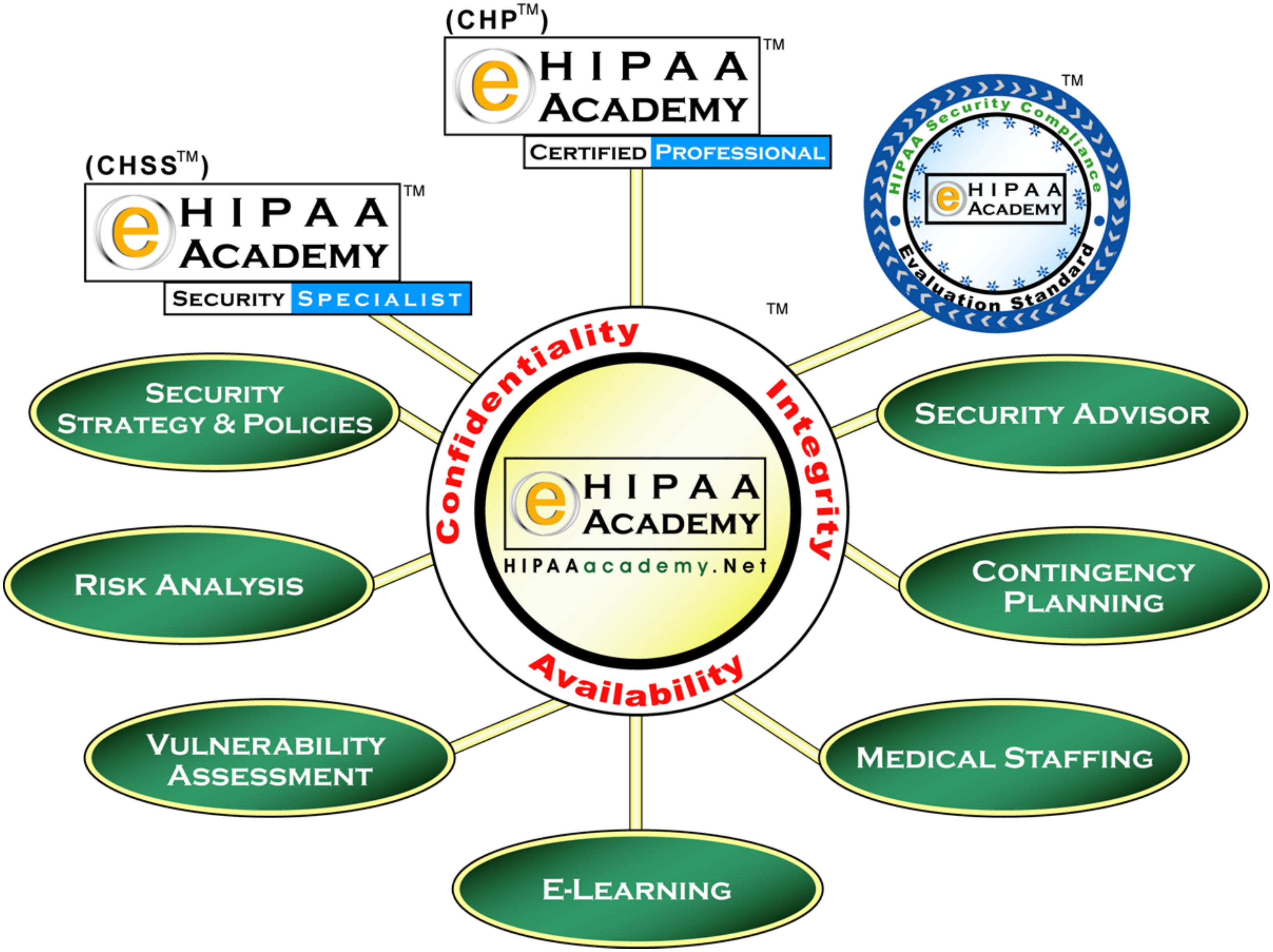
World-Class Information Security Regulatory Compliance Services

Endorsed by the American Hospital Association (AHA) Solutions, HIPAA Academy delivers compliance solutions across the United States every day. Our deep knowledge of legislations such as HIPAA, FISMA, Sarbanes-Oxley and other regulations is substantiated with hands-on experience implementing technical solutions in the industries we serve.

The HIPAA Academy introduced the industry's first credentials for HIPAA skills certification: CHP™ and CHSS™. We are excited to have successfully completed many engagements with a variety of organizations including hospitals, long term care, state, county governments, and several others.

HIPAA Academy's client list includes esteemed organizations such as HCR Manor Care, U.S. Army, U.S. Air Force, U.S. Department of Homeland Security, hospitals and clinics, several state governments, including Oregon, Iowa and Illinois.

Talk to us about your specific requirements and we will tailor a solution that will meet your business objectives.



(CHP™)

HIPAA ACADEMY™ CERTIFIED PROFESSIONAL

(CHSS™)

HIPAA ACADEMY™ SECURITY SPECIALIST

HIPAA Security Compliance Evaluation Standard™ HIPAA ACADEMY

Confidentiality Integrity Availability™

HIPAA ACADEMY

HIPAAacademy.Net

SECURITY STRATEGY & POLICIES

SECURITY ADVISOR

RISK ANALYSIS

CONTINGENCY PLANNING

VULNERABILITY ASSESSMENT

MEDICAL STAFFING

E-LEARNING

www.HIPAAacademy.Net

877.899.9974 16 & 17

HIPAA Security Compliance Audit for Evaluation Standard

The HIPAA Security Rule establishes very clearly the requirements for the Evaluation standard:

Evaluation Standard

Perform a periodic technical and non-technical evaluation to demonstrate and document compliance with the entity's security policy and the requirements of the HIPAA Security Rule.

Standards	Implementation Specifications	R = Required A - Addressable
Evaluation		R

As part of the Administrative Safeguards requirement, an organization must meet the requirements of the Evaluation standard.

The HIPAA Security Rule establishes very clearly the requirements for the Evaluation standard.

HIPAA Academy consultants will visit client site for HIPAA Security Compliance for Evaluation Standard. Our consultants will come back to our office and write the report offsite. The key deliverables of the report will be:

The HIPAAShield™ Evaluation Report will include information on the compliance status of the organization with all standards and implementation specifications of the HIPAA Security Rule. Only if the organization is found to be fully compliant with all aspects of the HIPAA Security Rule will the HIPAA Academy Seal of Compliance with the HIPAA Security Rule be authorized for use for a maximum period of twelve months from the date of issue.

In the event the organization was found to be not in compliance, then those areas will be specifically identified in the HIPAA Academy Report.

Recommended Next Steps with an Action Plan will identify critical areas that the organization must address expeditiously.

Client Testimonial

"I would like to thank your organization for the courtesy and professionalism your staff exhibited when interacting with MediNotes. We initially chose the HIPAA Academy because of your company's prominence and availability. Upon retrospect we were very fortunate to have chosen the HIPAA Academy. Here at MediNotes we found the HIPAA Academy to be extremely dynamic and responsive to our needs. The ultimate evaluation of our product was an easy process due to the prior input and suggestions from your company's staff. Your suggestions have really added value to our product and help us become HIPAA Complaint."

Don Schoen, CEO
MediNotes Corporation

Certified HIPAA Professional™ (CHP™)

HIPAA ACADEMY™ CERTIFIED PROFESSIONAL

The Certified HIPAA Professional™(CHP™) certification training helps you better understand HIPAA's Administrative Simplification Act as well as how to create a framework for initiating and working towards a blueprint for HIPAA compliance. From the CHP™ program you will learn the following about HIPAA:

- Step through how to plan and prepare for HIPAA compliance. HIPAA is about awareness first, assessment second and finally action focused on gaps identified.
- Review specific requirements and implementation features within each security category.
- Learn why HIPAA compliance is better focused as a business issue than as an IT issue, although IT will play a major role in implementing compliant systems.
- Examine how implementing HIPAA will affect the way healthcare entities organize and staff to achieve and monitor compliance with patient privacy/confidentiality needs.

Course Outline: http://www.hipaaacademy.net/HIPAA_Training/chpcourseoutline.html
Training Schedule: http://www.hipaaacademy.net/hipaatraining/training_schedules.html

Client Testimonial

"The dedication and passion that your team presented on a daily basis for the past five months has been outstanding. We were able to surpass our project goal by 6 percent and maintain our projected budget! This is a direct reflection of the flexibility of both your Management team and the on-site HIPAA Consultants performing the training."
Teri Cardinale
Training Specialist, State of Oregon

Certified HIPAA Security Specialist™ (CHSS™)

HIPAA ACADEMY™ SECURITY SPECIALIST

A core aspect of the Health Insurance Portability and Accountability Act (HIPAA) is to secure electronic medical records. In this HIPAA Security boot camp we examine all defined HIPAA security specifications and identify options and solutions available to secure health care entities.

The HIPAA security provision will result in substantial investment in e-business initiatives and deployment of security technology specifically in the health-care and insurance industries. The Certified HIPAA Security Specialist™ (CHSS™) training helps you understand the core elements for defining the framework towards HIPAA's security compliance.

The program flow and content accounts for the three security domains defined within the HIPAA Security Rule. The HIPAA security domain topics are addressed in the context of the required implementation specifications and associated security technologies and policies. Each lesson is focused with health care examples, templates and solutions that will be valuable as your organization considers options to secure the enterprise.

Course Outline: http://www.hipaaacademy.net/HIPAA_Training/chsscourseoutline.html
Training Schedule: http://www.hipaaacademy.net/hipaatraining/training_schedules.html

HIPAA Academy/ ecfirst.com is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Nashville, TN 37219-2417. Telephone: 615.880.4200. Web site: www.nasba.org.

Client Testimonial

"We would strongly recommend the HIPAA Academy's CHSS™ program and the Seven Steps methodology to all Public Health Administrators, County and State governments and others. The program was delivered at a reasonable cost and it was tailored to meet all our requirements."
Mark Stevens, B.S., M.P.A.
President, Illinois Association of Public Health Administrators (IAPHA)

Vulnerability Assessment

It is recommended that network vulnerability analysis and penetration testing be included as part of the HIPAA required Risk Analysis. To address the area of vulnerability assessment, HIPAA Academy can assist your organization to create an inventory of all vital enterprise assets, systems and communications. An assessment checklist is created to document information about all critical systems and applications that process or store EPHI. The risk analysis team then specifically identifies:

- Key information technology systems and components for each critical asset
- Key systems and components for technology weaknesses/vulnerabilities that may be exploited

The HIPAA Academy uses a number of tools in assessing the vulnerability of an organization's systems and networks. Detailed reports are published by the HIPAA Academy based on analysis of the data collected from the various tools deployed both internally and as part of external penetration testing.

Client Testimonial

"The HIPAA Academy's 'Seven Steps to HIPAA Security Compliance™' methodology is an excellent framework to consider as member hospitals launch HIPAA security initiatives and activities. IHA is working closely with the HIPAA Academy to help members address HIPAA Security Rule requirements such as risk analysis, security policies and training."
Illinois Hospital Association (IHA)

HIPAA Security Strategy & Policies

HIPAA Academy has developed a suite of 58 security policies to help covered entities meet the challenges of creating HIPAA Compliant security policies. In this document we first focus on the process of developing a security strategy your framework for identifying the business requirements for information security. We identify the various types of security policies and procedures required for compliance with the legislation. Finally, templates are provided for security policies that are required by the legislation. These policies can be easily customized to meet the specific requirements of any health care organization.

Templates Components: http://www.hipaaacademy.net/HIPAASecurityPolicies/hipaaSecurityPolicyTemplatesComponents.html

Contingency Planning

Contingency plan is a HIPAA Security standard. The HIPAA requirement of the contingency plan standard is to establish policies and procedures for responding to an emergency that damages systems that contain electronic protected health information (EPHI). This includes business continuity planning process, business continuity planning framework, testing business continuity plans and updating business continuity plans. The HIPAA Academy can assist you efforts with initiatives in this area including:

- Conduct a Business Impact Analysis (BIA)
- Review of existing disaster recovery and contingency plan documents
- Development (enhancement) of all documents required to achieve HIPAA security compliance in this Standard including Emergency Mode Operations Plan, Data Backup Plan and others

Client Testimonial

"This class was extremely helpful in understanding and preparing for the HIPAA Compliance. As a CISSP with CE requirements, I will highly recommend this class to others. The material and Instructor were great. "
Chris Feeney, CISSP, Computer Services Partners, Inc.

Risk Analysis

An accurate and thorough Risk Analysis, as required by the HIPAA Security Rule, is a major undertaking for any organization. HIPAA Academy consultants, with their expert knowledge of the HIPAA regulations along with their experience consulting in a wide range of organizations, can complete such a project faster and easier than attempting a Risk Analysis "in-house."

A HIPAA Academy engagement, although completely customizable to your needs, most often address the regulation's requirements for Risk Analysis, Information System Activity Review, and Contingency Planning.

More information: http://www.hipaaacademy.net/consulting/riskanalysis.html

Client Testimonial

"The HIPAA Academy provides services across the United States, but we felt that we were a priority group being served. I am sure that this is indicative in all of the services they provide to other organizations. The staff of the HIPAA Academy has a strong grasp of HIPAA, combined with a common sense knowledge of how organizations work."
Patricia Anderson, PHR, Mid-Willamette Valley Senior Services Agency

Security Advisor

The HIPAA Security Advisor can assist your organization's HIPAA and InfoSec initiatives in the areas of:

- Risk Analysis
- Vulnerability Assessment
- Development/customization of Security Strategy and Policies
- Training for Members of the HIPAA Security Team
- Security Training for Managers
- Security Audit and Evaluation
- Development of InfoSec and HIPAA Security RFPS
- Security Vendor and Product Reviews

Retain a HIPAA Academy Security Advisor for as few as 2 days a month.
Get immediate access to experienced HIPAA security professionals, without a long term commitment.

More information: http://www.hipaaacademy.net/consulting/privacy_security_advisor.html

E-Learning

1) HIPAAShield™ Compliancy Training

HIPAAShield™ Compliancy Training is devoted to helping organizations meet the Administrative Simplification Act section 164.530(b)(1). This section requires employers to provide HIPAA awareness and "Job Role" policy training. Our course is designed to reach all level of employees from providers to billing clerks to housekeeping.

More information: http://www.hipaaacademy.net/HIPAA_Training/eLearning/hipaaShieldhipaaTraining.html

2) HIPAA Security Training For End Users

This course is designed for all health care, insurance, and Business Associate employees who have access to patient records, which are governed under the final Security Rule of HIPAA. This group includes, but is not limited to, admissions, billings and nursing, management, physicians, social workers, case managers and clerks. This course focuses on security issues for patients and their records as defined by the HIPAA standards. It teaches the safeguards that staff need to be aware to appropriately secure all electronic Protected Health Information (EPHI).

More information: http://www.hipaaacademy.net/HIPAA_Training/eLearning/hipaaELearningMidsize.html

Clients

- ADASBCC
- Advocat Diversicare
- Advocate Health Care
- AT&T
- Baptist Saint Anthony
- Blessing Hospital
- Blue Cross Blue Shield Blue Care Network of Michigan
- Condell Medical Center
- Delta Dental
- Delta Health Systems
- Edward Hospital and Health Services
- Extendicare
- Greater Newport Physicians at Hoag Hospital
- Halifax Regional Medical Center (HRMC)
- Hanford Environmental Health Foundation
- Harborview Medical Center
- HCF Management, Inc.
- HCR ManorCare
- Hewlett-Packard
- Huntington Hospital
- Illinois Association of Public Health Administrators
- IntegraMed America
- Iowa Nurses Association
- Lancaster County of Nebraka
- Loyola University Health System
- MediNotes
- New Hanover Hospital
- Northwest Community Hospital
- Northwestern Memorial Hospital
- Olmsted Medical Center
- Passavant Hospital
- Principal Financial
- Provena Health
- Rehoboth McKinley Christian Hospital
- RSA Security
- Samaritan Hospital
- Sherman Hospital
- Sprint
- St. Anthony's Health Center
- State of Illinois, Dept. of Human Services
- State of Nevada, Dept of Human Resources
- State of Oregon, Dept. of Human Services
- TransHealth
- U.S. Air Force
- U.S. Army
- U.S. Department of Veterans Affairs
- University of Pittsburgh Medical Center
- VeriSign
- Wells Fargo
- William Beaumont Army Medical Center - U.S. GOV

Valued Partners

- American Hospital Association (AHA) Solutions
- RSA Security
- Train For HIPAA
- Prometric
- Course Technology
- Computer Associates
- CompTIA
- Illinois Hospital Association
- MeasureUp

ENDORSED BY THE AMERICAN HOSPITAL ASSOCIATION™